

# **EXHIBIT A**

# **EXHIBIT B**

Expert Report by Greg M. Cancilla and Evan R. Fuest  
from RVM Enterprises, Inc.

September 4, 2020

IN THE UNITED STATES DISTRICT COURT  
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA  
DURHAM DIVISION  
CIVIL ACTION NO: 1:16-cv-1174

NORTH CAROLINA MUTUAL LIFE )  
INSURANCE COMPANY, a North )  
Carolina Corporation, )  
)  
Plaintiff, )  
)  
v. )  
)  
STAMFORD BROOK CAPITAL, LLC, )  
a Delaware limited liability )  
company, *et al.* )  
)  
Defendants. )

Expert Report by Greg M. Cancilla and Evan R. Fuest  
from RVM Enterprises, Inc., an XDD Company  
September 4, 2020

## Table of Contents

Exhibits Enclosed.....	3
Background and Qualifications.....	4
1. Gregory M. Cancilla	
2. Evan R. Fuest	
Introduction and Summary .....	6
Evidence Considered.....	8
Examination.....	12
Conclusion.....	21

I. Exhibits Enclosed

*Exhibit 1.* Court order to Defendant to provide access to his electronic devices to RVM for forensic preservation and examination.

*Exhibit 2.* List of devices in the Defendant's possession ("the electronic device list").

*Exhibit 3.* Spreadsheet containing web browsing history from the Defendant's computer.

*Exhibit 4.* Preservation of screenshots of sites visited by the Defendant.

*Exhibit 5.* Spreadsheet containing Event Logs revealing prompts for deletion of data in Microsoft Outlook.

*Exhibit 6.* Report of a text message conversation with IT about deleting emails.

*Exhibit 7.* List of items in the Defendant's Windows Recycle Bin.

*Exhibit 8.* Multiple artifacts cross corroborating the download, installation and execution of the anti-forensic software Eraser.

*Exhibit 9.* Windows 10 Telemetry data logging the program Eraser as open for a span of 7 Days after initial execution.

*Exhibit 10.* Curriculum Vitae of Gregory Cancilla.

*Exhibit 11.* Curriculum Vitae of Evan Fuest.

## II. Background and Qualifications

This report was prepared by Gregory M. Cancilla ("Cancilla") and Evan R. Fuest ("Fuest").

I. My name is Gregory M. Cancilla. I am over 21 years of age.

I am a Certified Computer Forensic Engineer and am the Director of Forensics for RVM Enterprises ("RVM"). I have been employed in that capacity by RVM since April 2010. I received a bachelor's degree in business administration and computer science from the University of Toledo in 1999, and I am an EnCase (EnCE) and AccessData (ACE) Certified Examiner. I have been appointed as a neutral officer of the court for the purposes of preserving and producing electronic data on multiple occasions, and I regularly speak and publish on issues relating to computer forensics and the preservation of electronic data. I have personally conducted and overseen numerous digital forensic examinations of hundreds of computer hard drives, mobile phones and tablets, Cloud-based servers, and other media.

A true and accurate copy of my curriculum vitae is attached hereto as Exhibit 10. I am being compensated for my work on this engagement at my normal hourly rate of \$325/hour for forensic analysis and my normal hourly testimony rate of \$550/hour.

I am not affiliated with any party to this action.

2. My name is Evan R. Fuest. I am over 21 years of age.

I am an expert in the field of computer forensics. I am a Computer Forensics Engineer at RVM where I have been employed since October 2011. In my role as a Computer Forensics Engineer, I have had primary responsibility for several hundred digital forensic engagements and have first-hand knowledge in the collection, preservation, analysis and production of electronically stored information from digital media. I have received training and earned industry certifications, including AccessData Certified Examiner (ACE), CompTIA A+ (A+), and Cellebrite Certified Logical Operator (CCLO). I have provided testimony for my services in numerous engagements.

A true and accurate copy of my curriculum vitae is attached hereto as Exhibit 11. I am being compensated for my work on this engagement at my normal hourly rate of \$325/hour for forensic analysis and my normal hourly testimony rate of \$550/hour.

I am not affiliated with any party to this action.

### III. Introduction and Summary

1. On December 21, 2017, RVM Enterprises, Inc. ("RVM") was retained by Squire Patton Boggs for the purposes of forensically collecting data directly from Bradley C. Reifler ("Reifler"), founder and chief executive officer of multiple New York-based financial services firms in connection with a bankruptcy adversary proceeding involving North Carolina Mutual Life Insurance Company ("NCM").
2. On December 28, 2017, the court entered an order (the "December 28, 2017 Order"), Exhibit 1, ordering Reifler to provide access to his electronic devices to RVM for forensic preservation and examination. Specifically, the Order required RVM to "(a) conduct a forensic examination and capture of all content associated with [Reifler's] Electronic Devices and Email Accounts (collectively, the 'Data') and (b) process, collect, and maintain a full set of the Data." Exhibit 1 at 3. Pursuant to the December 28, 2017 Order, on January 5, 2018, Reifler provided a list of devices in his possession, Exhibit 2 ("the Electronic Device List").
3. While RVM's initial efforts to collect electronically stored information ("ESI") from Reifler were met with threats and hostility by Reifler, after several attempts, RVM was able to inspect and preserve full forensic images of some of the devices provided as part of the Electronic Device List.
4. RVM has now provided copies of the Data collected in conjunction with its initial engagement with Squire Patton Boggs for this action. RVM understands



that the same documents and information collected for Reifler's bankruptcy adversary proceeding are relevant to this matter.

5. This report is a summary of RVM's findings regarding the preservation attempts, forensic analysis, and reporting from forensic images of devices that RVM collected from Reifler as part of the December 28, 2017 Order.
6. All opinions offered in this report are offered to a reasonable degree of certainty.

#### IV. Evidence Considered

1. Consistent with the December 28, 2017 Order, on January 5, 2018, Cancilla spoke with Reifler on the phone about the Data in his possession, custody, or control, or that he has or can obtain access to for the purpose of full forensic examination and data collection.
2. Reifler informed Cancilla that Reifler would only provide access to a subset of Data in his possession, custody, or control, i.e., those that contained only "personal," vs. "business" data.
3. Reifler also informed Cancilla that Reifler possessed electronic devices at his "150-acre farm," but was unwilling to identify the devices or provide them to RVM for collection.
4. However, during the January 5, 2018 phone conversation with Cancilla, Reifler did agree to provide RVM access to some of his Data on January 10, 2018.
5. On January 10, 2018, pursuant to the December 28, 2017 Order, Fuest attempted to image Reifler's Data at Reifler's office.
6. Reifler only permitted Fuest access to one phone and parts of two computers -- not all the electronic devices in the list provided to RVM (Exhibit 2). One of the computers had three hard drives, and the other computer had no hard drives.
7. After Fuest collected an image of the phone and only one hard drive, but before Fuest could collect the Data from all of Reifler's electronic devices that had been made available that day, Reifler aggressively threatened Fuest and then kicked him out of his office.

8. On February 6, 2018, Cancilla was informed that the court in the bankruptcy adversary proceeding issued another order, entitled Order Finding Defendant in Contempt and Imposing Sanctions.
9. On February 14, 2018, RVM sent a courier to Reifler's offices and collected two computers.
10. As a result of multiple collection efforts and using widely accepted digital forensic practice and procedure, RVM collected a forensic image of a mobile phone and forensic images of hard drives in two desktop computers. The facts in this report are specifically based on the data extracted, analyzed, and reported on from the "working copies" of forensic images taken of Reifler's custom computer, with multiple hard drives, and mobile phone ("the Forensic Images").
11. The Forensic Images collected by RVM were verified using MD5 and SHA256 derived cryptographic hash values. The table below lists the Forensic Images that RVM considered for its facts included in this report.

Description	Type	Serial Number	Evidence Hash Value
"Debtor's work computer Custom built" Hard Drive 1	Hard Drive	WMC4M0935075	MD5: 57c477524b826975f535bb25e4abbfc3
"Debtor's work computer Custom built" Hard Drive 2	Hard Drive	160952441404	MD5: 3f37006442ee8e9f41337f28dd15c95e
"Debtor's work computer Custom built" Hard Drive 3	Hard Drive	2G1602110194	MD5: 4185f206a6ac8650906a95322eb03b83
Apple iPhone 7+	Mobile Device	FCLT1AH9HPY7	SHA256: 61CA7A1A333DEAD6AC9773930402DD11660E5383E6D7215A9FS3D16E4AC4C578

12. Other media collected or examined by RVM but not considered for examination in this report are in the table below.

Description	Type	Serial Number/Provider	Evidence Hash Value / Comment
"Assistant's Work computer HP KW4600" SN: 2UA85201H2	Hard Drive	9VP8H9NT	MD5: 1542091aabe0e4ac2a53cd796152c1d3
Debtor's personal computer HP, Model EN345UT	-	-	No Hard Drives in the computer.
Debtor's Apple watch	Mobile Device	359436081022314	Device not supported for collection.
breifler@forefrontgroup.com	Webmail	Microsoft Outlook.com	MD5: b601014878401b02cfdda513e1c6369a
breifler@gmail.com	Webmail	Google Gmail	MD5: a1b972eeaac267733cb9a62bebfb44f2
breifler@forefrontgroup.com	Cloud Storage	Dropbox	MD5: 121ff3989ac01def72588978d38c2394
breifler@gmail.com	Cloud Storage	Dropbox	Empty
breifler@gmail.com	Cloud Storage	Google Drive	MD5: 2bd7bd04b4aha6e9805c0e06d59541da

13. The primary analysis and conclusions that RVM presents are the result of examination conducted using industry standard forensic tools and software outlined below.

- Tableau TD3 Forensic duplicator
- Cellebrite UFED4PC 6.4.1.599
- Cellebrite UFED Physical Analyzer 7.0.0.108
- AccessData Forensic Toolkit (FTK) v6.4

- Magnet Axiom version 1.2
- Guidance Encase v8.0.5
- Aid4Mail version 4.61

## V. Examination

1. The examination that RVM performed of the Forensic Images was specifically tailored to identify and determine whether there was evidence that Reifler had destroyed, or attempted to destroy, ESI, with specific attention paid to ESI that is or may be relevant to the bankruptcy adversary proceeding, and therefore, this matter.
2. RVM employed a framework for analyzing the Forensic Images that builds a chronology of events that are grounded by standard digital forensic artifacts and maintain historical actions and events routinely recorded by Reifler's devices through the ordinary course of business.
3. RVM then took an in-depth look at the data contained within the digital forensic artifacts to highlight simple yet common terms that may be related to the destruction of ESI. The terms include erase, destroy, recycle, wipe, and delete.
4. Additionally, RVM examined locations such as the recycling bin and event logs for records of deletion activity.
5. RVM's examination revealed a number of references to and records of activity that are directly related to the destruction of ESI and recorded as part of Reifler's: (1) Web History, (2) Event Logs, (3) Text Messages (4) Recycling Bin Items, and (5) Application-related Metadata, among others.
6. RVM viewed the web history, event logs, text messages, recycling bin items and application-related metadata mindful of the December 28, 2017 Order requiring that Reifler provide access to his electronic devices, as well as the

dates by which Reifler was required to provide forensic images of his devices, January 10, 2018. Viewing all of the data and information collectively demonstrates that Reifler took deliberate action to delete and/or remove relevant ESI from his devices.

### **Web History Analysis**

7. The URLs and Page Titles from the Web Browsing History included as part of Exhibit 3 reveal that, on multiple occasions, including after knowing about his obligation to preserve ESI, Reifler searched phrases like "permanently delete deleted files on windows ssd" and visited web pages containing tutorials and tools that specifically walk through how to erase and overwrite files so that they are no-longer recoverable. Specifically, Reifler took the following actions:

- December 20, 2017:
  - 8:50 a.m.: Reifler performs a Google search for "erasing phone email and text history."
  - 8:50 a.m.: Reifler visits a webpage for [ios.gadgethacks.com](http://ios.gadgethacks.com), titled "How to Permanently Delete Text Messages on Your iPhone."
  - 10:38 a.m.: Reifler performs a Google search for "how to erase all emails on iphone."
  - 10:46 a.m.: Reifler visits a webpage for [www.imore.com](http://www.imore.com) titled "How to Trash All Your Email on Your iPhone, iPad, or iPod touch."
- January 2, 2018:
  - 9:53 a.m.: Reifler performs a Google Search for "erase deletes."
  - 9:54 a.m.: Reifler visits a blog posted to [www.raymond.cc](http://www.raymond.cc) titled "10 Free Tools to Permanently Delete Files and Prevent Data Recovery."
  - 10:00 a.m.: Reifler performs a Google search for "permantly [sic] delete deleted files on windows ssd."



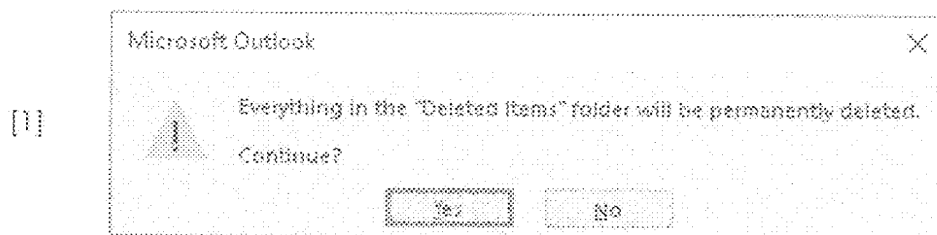
- o 10:00 a.m.: Reifler visits a webpage for [www.makeuseof.com](http://www.makeuseof.com) titled "How to Securely Delete Files from your HDD or SSD in Windows."
- o 10:09 a.m.: Reifler visits a webpage for [www.tomshardware.com](http://www.tomshardware.com) titled "Deleting Files/Data from SSD Permanently."
- o 10:11 a.m.: Reifler visits a webpage for [www.howtogeek.com](http://www.howtogeek.com) titled "Why Deleted Files Can be Recovered, and How You can Prevent It." The webpage explains the benefits of a TRIM-enabled solid-state hard drive for those seeking to permanently delete information. Specifically, the webpage provides that "when you use a TRIM-enabled SSD (all modern SSDs support TRIM), deleted files are removed immediately and can't be recovered."
- o 10:12 a.m.: Reifler performs a Google search for "TRIM-enabled SSD for windows 10."
- o 10:14 a.m.: Reifler visits a webpage for [www.windowcentral.com](http://www.windowcentral.com) titled "How to Ensure TRIM is Enabled on Windows 10 to Keep an SSD at Top Performance."
- o 10:23 a.m.: Reifler performs a Google search for "permanently delete deleted files on windows ssd."
- o 10:23 a.m.: Reifler visits a webpage for [www.zdnet.com](http://www.zdnet.com) titled "How to really erase any drive -- even SSDs -- in 2016."
- o 10:59 a.m.: Reifler visits a webpage for [www.pcworld.com](http://www.pcworld.com) titled "You Can Securely Wipe Your Files, Hard Drive or SSD with One of these Free Utilities."
- o 11:01 a.m.: Reifler visits a webpage for [www.easeUS.com](http://www.easeUS.com) titled "How to Securely Erase or Wipe SSD in Windows 10."
- o 1:24 p.m.: Reifler performs a Google search for "permanently deleting deleted emails on ssd."
- o 1:25 p.m.: Reifler visits a webpage for [www.fieldguide.gizmo.com](http://www.fieldguide.gizmo.com) titled "How to Safely Delete Private Data Forever." The webpage touts the permanent deletion ability of a third-party software application called "Eraser." Specifically, the webpage provides that "Eraser is a simple but effective tool that's been around a long time on Windows. Point it towards a file or folder and it overwrites it with random data that should be enough to stop it from ever coming back."



- See Exhibit 4 demonstrating some of the webpages visited by the web browser on Reifler's computer that are related to the destruction of ESI and are stored as screenshots with metadata related to the point in time collection of the webpages.

### Event Log Analysis

8. The "Payload" information as stored in the Event Logs on Reifler's computer included as part of Exhibit 5 contain multiple entries with text such as 1. "Microsoft Outlook Move "North Carolina Mutual" to your Deleted Items folder?" and 2. "Alert: Everything in the "Deleted Items" folder will be permanently deleted." These are confirmation prompts from Microsoft Outlook (1) requesting Reifler to confirm if a folder should be moved to the Deleted Items Folder and (2) providing a warning that emptying the Deleted Items folder will result in the permanent deletion of its contents.
9. The message prompt "Deleted Items folder will be permanently deleted" [1] is displayed by Microsoft Outlook when a user deliberately right clicks on "Deleted Items" and selects Empty Folder [2].



10. The prompt explicitly states "permanently deleted" when the user accepts the prompt by clicking "Yes" then any messages that are in the folder are deleted and can become overwritten by new data. As the data is overwritten, the chances of recovery diminish and data that has been completely overwritten is not recoverable.

11. RVM's analysis of the Event Logs from the Forensic Images demonstrates the following:

- a. December 28, 2017 at 12:45 p.m.: Reifler deleted or attempted to delete a Microsoft Outlook email folder titled "Water Joel emails."
- b. December 28, 2017 at 12:46 p.m.: Reifler deleted or attempted to delete a Microsoft Outlook folder titled "Joel."
- c. December 28, 2017 at 1:01 p.m.: Reifler deleted or attempted to delete a Microsoft Outlook folder titled "North Carolina Mutual."
- d. December 28, 2017 at Multiple Times: On 9 other occasions on December 28, 2017, Reifler deleted or attempted to delete everything in the "Deleted Items" folder of Microsoft Outlook, including for the first time at 12:22 p.m.
- e. January 2, 2018 at 9:46 a.m.: Reifler deleted or attempted to delete a Microsoft Outlook email folder titled "Summit Trust; George and K . . ."
- f. January 2, 2018 at 2:46 p.m.: Reifler deleted or attempted to delete a Microsoft Outlook email folder titled "Inbox."

g. Unknown Dates Post-December 19, 2017: Between December 19, 2017 and February 14, 2018, Reifler deleted at least 2,545 emails. Among the deleted emails is (1) an email with multiple PDF attachments, one of which appears to be an email conversation from December 3, 2014 from Reifler to Fickes, which Reifler forwarded to himself on January 16, 2018 and (2) a January 9, 2018 email Reifler received from Margaret Leszcznska, which attached multiple other emails including a November 3, 2014 email from Rodney A. Omanoff to Reifler and David Wasitowski with the Subject: "FW: OPERATING AGREEMENT FOR FOREFRONT TALKING CAPITAL INVESTMENT (FTCI)."

12. While RVM attempted to recover deleted emails, and paragraph 27(g) above describes some of the emails RVM recovered where Sent and/or Received dates remained intact, RVM cannot determine the full extent of what may have been deleted. RVM's recovery attempts resulted in some in-fact emails and a large amount of partially overwritten or unrecoverable email data. As described more fully in paragraphs 15–19 below, one way to overwrite data, including email data, on a hard drive and render it unrecoverable is through the download, installation, and execution of data destruction software, like Eraser.

#### **Text Message Analysis**

13. RVM also uncovered text message conversation between Reifler and Angel Santos. It is RVM's understanding that Angel Santos a member of Forefront II as found under the contact name "IT" in the address book stored on Reifler's

iPhone. In the conversation, appended as Exhibit 6, Reifler states "I want to delete all emails from 2016 onback".

#### **Recycling Bin Analysis**

14. Records from Reifler's recycling bin reveal that on January 2, 2018, Reifler moved hundreds of files from his computer's "Documents" and "Downloads" folders to the computer's recycle bin, including items with the following file names:

- a. Investment Advisory Agreement Steve Ficus [sic];
- b. Port Royal Investments;
- c. Review of NCM Proposal;
- d. FIT Holdings with Descriptions;
- e. Copy of NCM MaxRe Calculation 123116\_MaxRe.xlsb.

Exhibit 7 contains a listing of the files moved to Reifler's computer's recycling bin and the date they were moved. 96% of the files in this listing were placed in the recycling bin on January 1, 2018.

#### **Application-Related Metadata Analysis**

15. A long list of application-related records extracted from system logs, prefetch files, stored registry keys, and web browser records is included as Exhibit 8 and is related to the download, installation and execution of data destruction software named Eraser.

16. Under the Help section of Eraser's website, the following message details the nature of the program and its user-friendly interface.

## "OVERVIEW

*Eraser is an advanced security tool which allows you to completely remove sensitive data from your disk drives by overwriting it several times with carefully selected patterns. You can drag and drop files and folders to the program, setting arbitrarily complex schedules and any number of targets, or use the convenient Windows Explorer shell extension.*

*All the patterns used for overwriting are based on published standards by either researchers or government agencies and they are selected to effectively remove the magnetic remnants from the hard disk making it impossible to recover the data. These methods include*

*Peter Gutmann's paper Secure Deletion of Data from Magnetic and Solid-State Memory*

*National Industrial Security Program Operating Manual of the US Department of Defense*

*Simple pseudorandom data.*

## USING ERASER

*Eraser, although being designed as an advanced security tool, has a user-friendly interface for users to design, schedule and execute tasks. The interface is therefore an integral part of the user's workflow and in this chapter we demonstrate the common tasks users expect of such a program."*

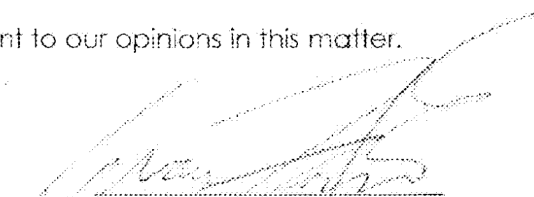
17. On January 2nd, 2018 Eraser was downloaded and installed to Reifler's computer as evidenced by the created date of the file Eraser.exe and the download history extracted from the Google Chrome web browser and event log records. Specifically,
- a. January 2, 2018 at 1:44 p.m.: Reifler begins downloading Eraser and installs Eraser to his computer;
  - b. January 2, 2018 at 1:50 p.m.: Reifler opens the Eraser program;
  - c. January 2, 2018 at 1:51 p.m. – 1:53 p.m.: Reifler opened the settings of Eraser and clicked the "Save Settings" button.
  - d. January 2, 2018 at 1:54 p.m. – 2:45 p.m.: No logs or records of deletion activity exist which is consistent with the Eraser program having been used.

18. On January 9th, 2018 Eraser was uninstalled from Reifier's computer one day prior to RVM's scheduled forensic collection of the devices listed in the electronic device list.
19. Records from the Windows 10's Telemetry data reveals that the Eraser software was opened and running for a period of 7 days – from the January 2, 2018 install to the January 9, 2018 uninstallation.

## VI. Conclusion

1. The forensic evidence, in combination with Reifler's actions, demonstrate to a reasonable degree of certainty that Reifler destroyed, and attempted to destroy, ESI, including ESI with file names and titles associated with the parties in this action. The forensic evidence shows that immediately preceding the December 28, 2017 Order, Reifler started performing Google Searches for how to permanently delete data, deleting items from his email account, and moved hundreds of files to the recycle bin. Reifler's intentional destruction continued by installing the Eraser software program in an attempt to remove information from his devices before the scheduled imaging was to occur by RVM. Then, in an attempt to cover up his deletion activities, Reifler uninstalled the Eraser software – the day before RVM was present at his offices for the imaging.
2. We reserve the right to supplement this report to the extent that we are provided with additional information relevant to our opinions in this matter.

  
Greg Cancilla  
9/3/2020

  
Evan Fuest  
9/3/2020

# EXHIBIT 11

to  
Expert Report of Greg M. Cancilla and Evan R. Fuest

**Exhibit 11:**  
**Curriculum Vitae of Evan Fuest**

Served native pdf file via email to david@wasitowski.com, breifler@gmail.com, and breifler@forefrontgroup.com on September 4, 2020.



## **Evan Fuest**

Computer Forensics Engineer  
[efuest@rvminc.com](mailto:efuest@rvminc.com) | [rvminc.com](http://rvminc.com)

### **Summary**

Evan Fuest, A+, ACE, CCLO is a certified Computer Forensic Engineer at RVM. He is versed and well trained in the preservation, identification, extraction, documentation and interpretation of digital data. Evan has several years of experience in the information technology field designing, administrating and facilitating complex data systems. Throughout his extensive career Evan has designed large scale backup and redundancy plans for firms seeking to ensure reliability and disaster recovery. Evan has completed a wide range of computer forensics and information technolgy training programs from renowned industry outfits, such as Access Data, Kcure Software, Microsoft, VMware, and participated in selected mathematic and computer science programs at private institutions where he continues to pursue additional degrees. As a forensic engineer, he has performed hundreds of digital forensics investigations, and reviews while maintaining an extensive career in information technology since entering the field in 2004. Evan holds a Bachelor's Degree in Economics from Drew University.

### **Education**

Drew University, Madison, New Jersey 2004-2008  
Bachelor's degree in Economics, minor Political Science

### **Certifications**

Comptia A+  
AccessData Certified Examiner (ACE)  
Cellebrite Certified Logical Operator (CCLO)  
Relativity E-Discovery Certified Administrator Training

### **Professional Associations**

Drew University Alumni Association  
High Technology Crime Investigation Association (HTCIA)

### **Select Speaking Engagements**

**Social Media Data Collection**, Kubasiak, Fylstra, Thorpe & Rotunno, P.C., Chicago, IL, November 9, 2013

**Digital Forensics of Social Media and the Cloud**, Clausen Miller, New York, NY, November 20, 2013

**Forensics of Social Media**, LawLine, December 14, 2013

RVM, Inc., 40 Rector St. New York, NY 10006 | Tel 800.525.7915

### **About RVM**

RVM provides cutting-edge legal technology, consulting and support services. RVM's team of experts includes industry savvy consultants, premier project managers and seasoned support personnel. RVM's team collaborates with each client to assess its litigation support needs, and can tackle the most demanding digital forensics, e-Discovery and e-Data processing assignments. RVM's proprietary e-Data processing software, Revelation, delivers consistent, repeatable, and defensible results. In turn, RVM's clients experience a more streamlined and less costly attorney review process. RVM enjoys Safe Harbor Certification and has conducted forensic collection and analysis both domestically and internationally. Since 1996, RVM's legal and corporate clients have enjoyed RVM's exceptional service and measurable results.

### **RVM's Core Competencies**

- ✧ Litigation Needs Analysis Consulting
- ✧ ESI Solutions
- ✧ Forensics (Data Collection & Analysis)
- ✧ e-Data Processing
- ✧ Online Hosting & Review
- ✧ Enterprise Content Management

RVM, Inc., 40 Rector St. New York, NY 10006 | Tel 800.525.7915